Amended claims

1. (Currently Amended) A system employed by an application for encoding URL link data for use in detecting unauthorized URL modification, comprising:

a link processor for processing URL data by

identifying an address portion of said URL,

encrypting said address portion of said URL,

incorporating~~,~~ said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string~~;~~ and

providing a key supporting decryption of said encrypted address portion, to a destination system; and

a communication processor for incorporating said processed URL data string into formatted data for communication to said destination system.

2. (Previously presented) A system according to claim 1, wherein

said link processor adaptively identifies said address portion as URL data either,

(a) lying between "http://" and a question mark "?" or

(b) lying between "http://" and a pound/number sign "#", in response to whichever of condition (a) and (b) is satisfied first.

3. (Original) A system according to claim 1, wherein said link processor

adaptively identifies said address portion based on the application associated with said URL.

4. (Original) A system according to claim 3, wherein said link processor

adaptively uses (a) an address portion for ASP (Active Server Page) applications comprising a SERVER_NAME and SCRIPT_NAME and (b) an address portion for a non-ASP applications comprising a SERVER_NAME, SCRIPT_NAME, and PATH_INFO.

5. (Original) A system according to claim 1, wherein said link processor

compresses said address portion of said URL prior to encryption and incorporation into said processed URL data string.

6. (Original) A system according to claim 5, wherein said link processor

converts said address portion of said URL to lower case before compression.

7. (Original) A system according to claim 5, wherein said link processor compresses said address portion using at least one function from (a) a hash function, (b) another compression function.

8. (Previously presented) A system according to claim 1, wherein said link processor

incorporates at least one of, (a) a session identifier, identifying a particular session of user initiated operation of said application and (b) an encrypted patient identifier, into said processed URL data string.

9. (Original) A system according to claim 8, wherein said link processor

incorporates said session identifier into said processed URL data string by formatting said session identifier into a data field including said session identifier and encrypted address separated by a colon (that is, session identifier:encrypted address).

10. (Original) A system according to claim 1, wherein said link processor

concatenates said address portion of said URL together with data associated with a personal record to form a data element, and

encrypts said data element for incorporation into said single processed URL data string.

11. (Original) A system according to claim 10, wherein

said data associated with a personal record is at least one of, (a) a patient identifier, (b) a user identifier, (c) an encounter identifier and (d) an observation identifier.

12. (Currently Amended) A system according to claim 1, wherein

said link processor ~~encrypts~~ encodes said address portion of said URL using an RSA (Rivest Shamir Adleman) MD5 compatible hashing ~~algorithm~~ function.

13. (Currently Amended) A system employed by an application for encoding URL link data for use in detecting unauthorized URL modification, comprising:

a link processor for processing URL data by

identifying an address portion of said URL,

encrypting said address portion of said URL,

incorporating, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form and a session identifier identifying a user session of computer operation, into a single processed URL data string; and

a communication processor for incorporating said processed URL data string into formatted data for communication to a request device.

14. (Previously presented) A system according to claim 13, wherein

said link processor compresses said identified address portion and encrypts said compressed address portion of said URL to provide said encrypted address portion and

said link processor converts said identified address portion to lower case prior to compressing said identified address portion using a hash function.

15. (Previously presented) A system employed by an application for decoding URL link data encoded for use in detecting unauthorized URL modification, comprising:

an input processor for receiving an encoded URL;

a link processor for processing said encoded URL by

identifying an encrypted address portion of said received encoded URL and a corresponding non-encrypted address portion of said received encoded URL,

decrypting said encrypted address portion of said URL to provide a decrypted URL address portion,

a validation processor for determining if said decrypted URL address portion has been subject to unauthorized modification by determining if said decrypted URL address portion is different to said corresponding non-encrypted address portion of said received encoded URL.

16. (Previously presented) A system according to claim 15, wherein said decrypted URL address portion is a first hash value, and

said validation processor,

applies a hashing function to said corresponding non-encrypted address portion of said received encoded URL to provide a comparison second hash value, and

compares said comparison second hash value with said first hash value, and upon a match determines a successful validation of said received encoded URL.

17. (Original) A system according to claim 15, wherein said link processor

identifies and extracts a session identifier from a non-encrypted portion of said received encoded URL.

18. (Original) A system according to claim 15, wherein

said decrypted URL address portion includes data associated with a personal record.

19. (Original) A system according to claim 18, wherein

said data associated with a personal record is at least one of, (a) a patient identifier and (b) a user identifier.

20. (Previously presented) A method employed by an application for encoding URL link data for use in detecting unauthorized URL modification, comprising the steps of:

identifying an address portion of a URL;

encrypting said address portion of said URL;

incorporating, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string;

providing a key supporting decryption of said encrypted address portion to a destination system; and

incorporating said processed URL data string into formatted data for communication to said destination system.

21. (Previously presented) A method employed by an application for decoding URL link data encoded for use in detecting unauthorized URL modification, comprising the steps of:

receiving an encoded URL;

identifying an encrypted address portion of said received encoded URL and a corresponding non-encrypted address portion of said received encoded URL;

decrypting said encrypted address portion of said received encoded URL to provide a decrypted URL address portion; and

determining if said decrypted URL address portion has been subject to unauthorized modification by determining if said decrypted URL address portion is different to said corresponding non-encrypted address portion of said received encoded URL.

22. (Previously presented) A method according to claim 21, wherein said decrypted URL address portion is a first hash value, and including the steps of

applying a hashing function to said corresponding non-encrypted address portion of said received encoded URL to provide a comparison second hash value, and

comparing said comparison second hash value with said first hash value, and upon a match determining a successful validation of said received encoded URL.